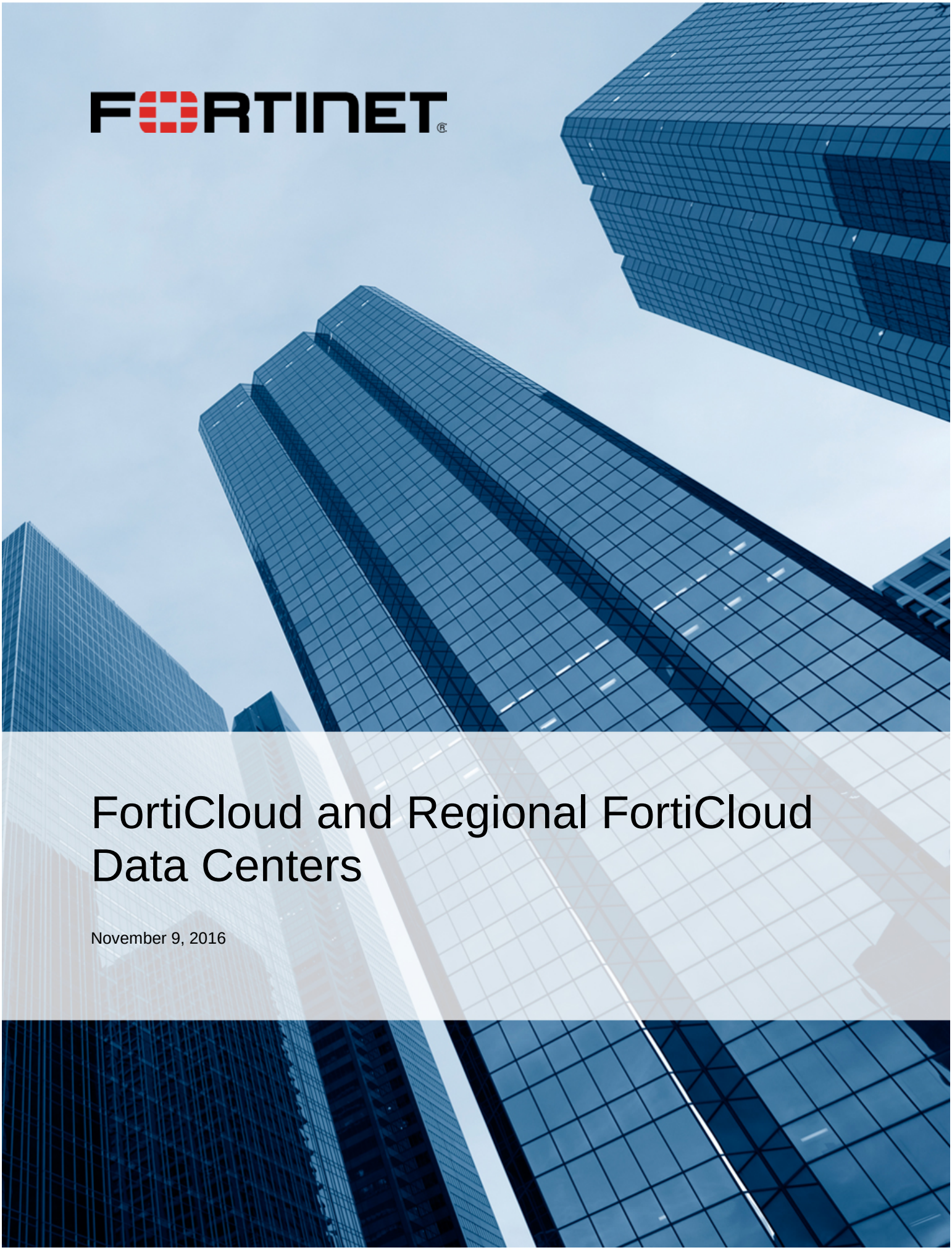

FortiCloud and Regional FortiCloud Data Centers

November 9, 2016

Where in the Cloud?

Cloud services and their competing definitions have been a relatively recent addition to the ever-expanding lexicon of computing terminology. We can at times find ourselves lost in these definitions and while this paper cannot hope to answer everyone's questions on Cloud Services it does serve to explain what exactly is FortiCloud.

It is important to understand the differing roles of cloud services, a management and reporting solution such as FortiCloud is reliant on the industry leading hardware deployed in the customer's physical network, a full cloud service such as FortiSandbox replaces hardware in the customer environment. Many cloud management systems are attempting to mask inferior hardware in the physical network while providing some analytics and capabilities in the cloud. Securing the cloud and the services within it is vital, but a significant number of attacks come from a local level and the hardware's ability to protect its information is critical.

Since its early beginnings back in 2007, FortiCloud has focused on bringing simplicity to a complex threat landscape; simplicity focused on provisioning, configuration for threat defense and visibility of the active threat landscape surrounding your IT infrastructure.

As a cloud based platform, FortiCloud provides a management platform for FortiGate, FortiWifi and FortiAP devices to deliver benefits that include:

- Support for FortiDeploy, to provide large scale device onboarding
- Simple, efficient and effective management
- Near real time identification of previously unknown threats
- Security analytics and visibility

As the popularity of this service has grown steadily, Fortinet have been growing the supporting infrastructure to deliver an ever more scalable solution which already has more than 200,000 devices under management (Oct 2016).

What is in the Cloud?

Storage of customer data within the cloud can be a sensitive topic; storage of security data and configuration information is always a sensitive topic. Recognizing the sensitivities involved, in December 2015 the FortiCloud team commissioned an additional Regional FortiCloud Datacenter, which came on stream in Q2 2016, geographically aimed at our European customer base. This new FortiCloud point of presence, while sharing the same architecture and FortiGuard infrastructure as our

initial center in North America, operates independently, to serve its target audience. All analysis, reporting, management and storage capabilities are provided locally with the benefit of full access to our global threat intelligence databases.
The geographic location not only isolates intercontinental data but also provides performance improvement with lower latency to the end device.

Why is it in the Cloud?

A key part of the FortiCloud service is the visibility it provides. This visibility is created by extensive analysis of log data that comes directly from the Fortinet managed devices connected to the cloud. At Fortinet we recognize the potential sensitivity of such log data and it is for this reason we ensure all log data is retained in the data center to which it was originally sent, there is no need to move this data around to complete the analysis performed by FortiCloud. The retention of this log data provides the framework for how the service is delivered to customers allowing a time based selection to be made, independent from the underlying storage requirements. This is not a service built around storage, but around various customer driven and compliance requirements.

Of course without a threat analysis component FortiCloud would be considered incomplete. We are able to leverage the significant benefits afforded by our FortiCloud Sandbox service within the regional data center. Delivered on dedicated servers this service complements the visibility of known threats by enabling the search for unknown threats. This threat analysis capability uses the same techniques available from the FortiSandbox product, delivering a comprehensive and award winning insight in to the content it is allowed to process. While the FortiSandbox cloud service necessarily needs to process files directly from a customer network these files, as with the log data, never leave the confines of our regional data center. The device sending the files to the sandbox appears in the FortiCloud homepage where an easy to navigate GUI allows access to a simple records view, organized into Malicious (Known/New), Suspicious, and Risk (High, Medium and Low). These are timestamped and shown with the relevant source and destination IP details along with the File Name for quick and easy information access. A Dashboard gives a graphical view of information such as processing time and top targeted hosts. Email alerts are sent to a designated recipient – the level of these alerts is customizable in the FortiCloud Sandbox GUI.

What are the facts?

- Regional European Datacenter for FortiCloud instance has been deployed and enabled
- Global FortiGuard Threat Intelligence Services are hosted in the same Data Center

- Fortinet devices configured to use the FortiCloud service dispatch their log data to the European Cloud based on their Geographical IP address. Meaning if you are in Europe you use the European data center
- Log data never leaves this datacenter.
- Any visibility and threat analysis is performed within the datacenter where the device's log data is stored.
- In FortiCloud* the Datacenter your FortiGate is logging/uploading to is indicated in the FortiCloud interface in the information section for each device.
- FortiCloud Sandbox is a service also now available within the Regional European Datacenter.
- While the selection of Regional Datacenters for log storage and sandbox threat analysis is automatic, Fortinet customer support can arrange for a manual transfer for any existing units sending their log data to other Datacenters.
- In FortiCloud*, when a Wireless network is setup, the user is given a choice which Datacenter they want the access points to be managed from, corresponding log data is send to this same data center
- The free service retains and provides analysis for 7 days of logs.
- 1 year log retention and analysis available in 1-5 year service terms. Pricing is a sliding scale based on the size of the FortiGate – the larger the FortiGate the larger the log storage required.
- Free Contract allows uploads of up to 100 files a day (10 files for FortiOS 5.4.0 and below).
- 1 Year FortiCloud Sandbox device contract allows for up to 144,000 file uploads per day.

How secure are my files?

As part of our due diligence we made sure our European FortiCloud instance is hosted in a ISO27001:2005 certified datacenter. This certification encompasses access and security regulations. Only log files and sandbox submissions are ever sent from the FortiGates and FortiWiFis. The file types sent for submission can be set on the FortiGate. FortiAPs send logs and Wi-Fi statistics to FortiCloud.

Are my files sent to any other Datacenters?

No. If your FortiGate is logging to the European Datacenter, the files are never sent anywhere else. This also applies to Sandbox and AP functionality.

Who has access to the data in FortiCloud?

In the event of a customer support case being raised or other maintenance work needed, Fortinet Engineers may access the data in FortiCloud. Other than those specific circumstances no one else has access to the storage of your files.

*FortiCloud 3.1 due for release Q4/2016

How about the files sent to FortiCloud Sandbox?

The files sent to the FortiCloud sandbox are processed in exactly the same way as if the appliance was onsite in your premises. Any clean completed files are deleted within 72 hours. Any malicious/suspicious files are kept in FortiCloud Sandbox for a maximum of 60 days. Signatures are directly generated by our FortiCloud Sandbox system in our European FortiCloud instance. No files are ever shared outside of this instance. These signatures then form part of the optional FortiSandbox Database GUI option on the FortiGate

How about other compliance and certifications?

We are constantly striving to make sure FortiCloud delivers the best service to users and as part of this we have ongoing reviews of processes and implement new certifications as they become relevant. If there is something specific, please reach out to your local team to discuss where we can provide information on demand. We are constantly working to expand the reach of the ISO27001:2005 and other certifications to encompass and drive our processes and controls.

In Summary

With the addition of a Regional European Data Center, with full access to our Global Threat Intelligence data, Fortinet provides the performance, convenience and reassurance of local cloud services whilst expanding the reach of the security fabric.

Of course, Fortinet cloud service offerings do not start and end with FortiCloud, we also provide a comprehensive email gateway service, FortiMail Cloud, and a wide range of cloud based technologies that can secure your own datacenter infrastructures.